

The Invention Claimed Is:

1. A method of operating an electronic lock box system, said method comprising:

5 (a) providing at least one electronic lock box having a secure compartment therein, a first computer circuit, a first memory circuit, a first device reader port, and a first data entry apparatus;

(b) providing a processing apparatus having a second computer circuit, a second memory circuit, a second device reader port, and a second data entry apparatus;

10 (c) providing a portable memory device having a third memory circuit, and at least one electrical conductor for communicating with a device reader port;

(d) at said second computer circuit:

15 (i) determining a first present epoch time, determining a predetermined epoch time window for which a portable memory device will be valid, determining a first cryptographic seed value for use with a data encryption function, and determining a user's first identification code;

(ii) using said data encryption function, calculating a diversified value based upon both said first cryptographic seed value and said user's first identification code;

(iii) coupling said portable memory device to said second device reader port, and communicating said diversified value to said portable memory device;

20 (e) at said at least one electronic lock box:

(i) coupling said portable memory device to said first device reader port, and communicating said diversified value from said portable memory device to at least one of said first computer circuit and said first memory circuit;

25 (ii) determining a second present epoch time, determining a second cryptographic seed value; and determining a user's second identification code from a manual entry at said first data entry apparatus;

(iii) using said data encryption function, decrypting said first diversified value based upon said second cryptographic seed value, resulting in a third identification code; and

30 (iv) comparing said user's second identification code and said third identification code, and if they match, permitting access to said secure compartment.

2. The method as recited in claim 1, wherein said user's second identification code will match said third identification code if the portable memory device is coupled to said first device reader port within said predetermined epoch time window.

5 3. The method as recited in claim 1, wherein said step of determining a first cryptographic seed value comprises: dividing said present epoch time by said predetermined epoch time window.

10 4. The method as recited in claim 1, wherein said data encryption function comprises one of: (a) a message digest function and a pseudo-random cryptographic key generator, (b) a random number generator algorithm, (c) a linear congruential random number generator (LCG) algorithm, and (d) a symmetric key encryption algorithm.

15 5. The method as recited in claim 1, wherein said step of determining a second present epoch time involves adjusting said present epoch time, based upon an ambient temperature at said at least one electronic lock box.

20 6. The method as recited in claim 1, wherein said portable memory device comprises one of: (a) a smart card; (b) a data key, and (c) a USB-compatible memory device.

25 7. A method of operating an electronic lock box system, said method comprising:
 (a) providing a central database computer and an electronic lock box at a second physical location;

 (b) encrypting, at a first real time, a user's identification number using a first encryption seed value that is known only to said central database computer and to said electronic lock box, wherein said first encryption seed value is time dependent;

 (c) storing said encrypted user's identification number on a portable memory apparatus at said central database computer;

30 (d) transferring said encrypted user's identification number from said portable memory apparatus to said electronic lock box;

 (e) decrypting, at a second real time, said encrypted user's identification number using a second encryption seed value, thereby resulting in a decrypted ID value;

(d) comparing said decrypted ID value to data entered on a keypad at said electronic lock box, and if the data matches said decrypted ID value, allowing access to a secure compartment within said electronic lock box.

5 8. The method as recited in claim 7, wherein said data entered on the keypad at said electronic lock box is equal to said user's identification number.

10 9. The method as recited in claim 7, wherein said first encryption seed value will be equal to said second encryption seed value, if said first real time and said second real time are both within a same predetermined time window.

15 10. The method as recited in claim 9, wherein said step of determining a first cryptographic seed value comprises: dividing a present epoch time by a predetermined time window in units of epoch time.

20 11. The method as recited in claim 7, wherein said encrypting step uses a data encryption function that comprises one of: (a) a message digest function and a pseudo-random cryptographic key generator, (b) a linear congruential random number generator (LCG) algorithm, and (c) a symmetric key encryption algorithm.

25 12. The method as recited in claim 7, wherein said step of decrypting said encrypted user's identification number, at a second real time, involves adjusting a present epoch time that corresponds to said second real time, based upon an ambient temperature at said at least one electronic lock box.

30 13. An electronic lock box apparatus, comprising:
 an electrical power source, a controller circuit, a secure compartment having an access member actuated by a prime mover apparatus, a manual data entry apparatus, and a device reader port; and
 a portable memory device that connects to said device reader port;
 wherein, said controller circuit is configured:

(a) to determine a present epoch time, to determine a predetermined epoch time window for which said portable memory device will be valid, to determine a cryptographic seed value for use with a data encryption algorithm;

(b) to read a first data value that is stored on said portable memory device;

(c) to decrypt said first data value using said data encryption algorithm, based upon said cryptographic seed value, thereby determining a second data value;

(d) to receive a user's identification code that is entered at said manual entry apparatus;

(e) to compare said user's identification code to said second data value; and

(f) if said user's identification code is equal to said second data value, to allow access to said secure compartment by actuating said prime mover apparatus to open said access member.

14. The electronic lock box apparatus as recited in claim 13, further comprising: central computer apparatus that includes a second device reader port; and

wherein said first data value is calculated by said central computer apparatus, which is configured to:

(a) determine a second present epoch time, determine said predetermined epoch time window for which said portable memory device will be valid, determine a second cryptographic seed value for use with said data encryption algorithm, and determine said user's identification code;

(b) using said data encryption function, calculate a diversified value based upon both said second cryptographic seed value and said user's identification code;

(c) using said second device reader port, to communicate said diversified value to said portable memory device.

15. The electronic lock box apparatus as recited in claim 14, wherein said user's identification code will match said second data value, if the present epoch time when the portable memory device is coupled to said device reader port, and if the second present epoch time when the central computer calculated said diversified value, are both within a same predetermined epoch time window.

16. The method as recited in claim 13, wherein said portable memory device comprises one of: (a) a smart card; (b) a data key, and (c) a USB-compatible memory device.

17. An electronic lock box apparatus, comprising:

5 an electrical power source, a controller circuit, a secure compartment having an access member actuated by a prime mover apparatus, a manual data entry apparatus, and a device reader port;

wherein, said controller circuit is configured:

10 (a) to determine whether said electronic lock box apparatus is presently in one of (i) a first, higher security state and (ii) a second, lower security state;

(b) if said electronic lock box apparatus is presently in said second, lower security state, access to said secure compartment may be obtained by a proper code, provided through said manual data entry apparatus; and

15 (c) if said electronic lock box apparatus is presently in said first, higher security state, access to said secure compartment may be obtained by a combination of a proper user's identification code, provided through said manual data entry apparatus, and by decrypting a diversified data value from a portable memory device, received through said device reader port.

20 18. The electronic lock box apparatus as recited in claim 17, wherein said code contains both security code information and identification data, thereby allowing said controller circuit to log and store unique identification information about a person who used the code, and wherein said stored unique identification information can later be retrieved from said electronic lock box apparatus and transferred onto a portable memory device.

25 19. The electronic lock box apparatus as recited in claim 17, wherein said code comprises one of: (a) a progressive code that changes over the passage of time; and (b) a static code that does not change over the passage of time.

30 20. The electronic lock box apparatus as recited in claim 17, wherein said second, lower security state is enabled when a predetermined "contractor mode" command is given to

said controller circuit by a particular authorized user who is authorized to issue said contractor mode command.

21. The electronic lock box apparatus as recited in claim 20, wherein said authorized user is identified by said controller circuit, based upon a predetermined portable memory device.

22. The electronic lock box apparatus as recited in claim 20, wherein said authorized user, when enabling said second, lower security state, may choose to set up the electronic lock box apparatus to one of:

(a) permit access to the secure compartment of said electronic lock box apparatus by an other user who provides a proper user's identification code, and who also connects a portable memory device to said device reader port which contains a correct diversified data value for a current epoch time window, in a mode similar to said first, higher security state; and

(b) prevent access to the secure compartment of said electronic lock box apparatus by an other user, even when said other user provides a proper user's identification code and also connects a portable memory device to said device reader port which contains a correct diversified data value for a current epoch time window.

23. The electronic lock box apparatus as recited in claim 22, wherein:

if said electronic lock box apparatus is set up so as to permit an other user to obtain access to said secure compartment while in its second, lower security state, then said authorized user may choose to set up the electronic lock box apparatus, upon such access of the secure compartment, to one of:

(a) automatically change a mode of said electronic lock box apparatus from said second, lower security state to the first, higher security state; and

(b) keep the mode of said electronic lock box apparatus in said second, lower security state.

24. The electronic lock box apparatus as recited in claim 20, further comprising a shackle member that is attachable to and detachable from said electronic lock box, said

shackle member being actuated by said prime mover apparatus as directed by said controller circuit;

wherein: if said authorized user operates said prime mover apparatus to detach said shackle from said electronic lock box at a time when the electronic lock box is in said second, lower security state, then said controller will automatically change a mode of said electronic lock box to said first, higher security state.

5